CONTINUATION

I, Trisha Kovac, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) currently assigned to the Detroit Division, St. Joseph Resident Agency. I have been an FBI Special Agent for nearly 11 years, and during that time have investigated numerous violations of federal law, including extortion and fraud cases.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 875(d) have been committed by Samantha Joyce BALMER. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

PROBABLE CAUSE

5. On February 5, 2020, a grand jury in the Western District of Michigan returned an indictment charging Samantha Joyce BALMER with making interstate communications with

intent to extort, in violation of 18 U.S.C. § 875(d). The following paragraphs contain facts underlying that offense that are pertinent to this warrant request.

6. On January 8, 2020 BALMER's victim (hereinafter "Victim"), contacted the FBI St. Joseph Resident Agency to report he was being blackmailed. Victim advised me that BALMER was formerly employed by the same company where he still worked. He admitted that in 2016, he had a consensual sexual encounter with BALMER at a company conference. On or about December 19, 2019, BALMER began sending him text messages on his cellular telephone demanding money. She threatened to expose the sexual encounter to Victim's wife and employer on social media, saying (among other things) that she would "wreck his life" unless he paid her $3,000.

7. Victim told me he took the threat seriously, at least in part because he was aware BALMER had made allegations of sexual assault against another coworker on social media. In addition, victim related that BALMER had been posting messages on her Facebook account about other men she claimed had harmed her.

8. On December 19, 2020, Victim paid BALMER $3,000 via PayPal.com. Shortly thereafter, BALMER demanded an additional $7,000; and then later demanded a month of his salary. The demand for additional money prompted Victim to contact local law enforcement, who referred him to the FBI.

9. On January 24, 2020, I met BALMER at a café in St. Joseph, Michigan, posing in an undercover capacity as Victim's attorney. I told BALMER that I was meeting her to facilitate payment, and that I would be asking her to sign a non-disclosure agreement. During our recorded conversation, BALMER increased her demand to $10 million in exchange for her silence, and

terminated the meeting. At that point, I disclosed my identity as an FBI agent, and placed BALMER under arrest.

10. In a post-arrest interview, BALMER told me she was desperate for money. She admitted extorting Victim because she knew he was wealthy, and believed she could get money from him in exchange for her silence. She encouraged me to look at her Facebook and Instagram accounts, which she told me she had recently reactivated. She specifically referenced a conversation on Instagram she had with an associate, who had encouraged her to seek a higher payout from Victim after receiving the original $3000. BALMER told me she had been "sexually abused numerous times by several men," or words to that effect.

11. Following the arrest, I reviewed the publicly available parts of BALMER's Facebook account, "samantha.balmer.33" account number 100004689164126. I located and downloaded a "Facebook Live" streaming video BALMER had posted on her way to meet me on January 24, 2020. In the video, BALMER spoke excitedly about how she was about to attend a meeting that would change her life.

12. I reviewed the publicly available "timeline" information from BALMER's Facebook profile, and saw that she had posted items each month from July 2019 to November 2019. Victim confirmed that BALMER had previously used Facebook Messenger to communicate with him before the extortion began.

13. I had conducted an open source search in mid-January 2020, but did not see an active Facebook profile for BALMER at that time. I observed, however, that BALMER's Facebook account was active again in late January 2020. Based on this information, it appears BALMER regularly maintained her Facebook profile; temporarily took down her account around

the time she was extorting Victim, and then reestablished her account sometime before the end of the January.

14. On January 29, 2020 I submitted a preservation request to Facebook, LLC, via the online law-enforcement portal, for account samantha.balmer.33, account number 100004689164126.

15. Based on BALMER's previous use of social media to facilitate extortion, her previous social media posts regarding alleged sexual assaults, and her admitted desperation for money, there is reason to believe Victim was not BALMER's only extortion target. I therefore believe BALMER's Facebook account may contain information regarding additional crimes, as well as additional evidence of the crime for which she is currently under indictment.

16. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

17. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user’s full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

18. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual

Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

19. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

20. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

21. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

22. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

23. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

24. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

25. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

26. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

27. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

28. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

29. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

30. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like

Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

31. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity

may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

32. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

34. Based on the foregoing, I request that the Court issue the proposed search warrant.

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Facebook. Because Facebook will then compile the requested records at a time

convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

36. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).